



[趋势科技成功案例]

网关设防 安全无忧

趋势科技 IWSA 1500 为安阳工商行政管理局严把网络“入口”安全

网络威胁每天都在层出不穷，攻击随时可能发生，而这些威胁中的 90%都来自于并不可信 Internet，而且由于缺乏网络防护的熟练技能，IT 人员的脑力和体力都被大量终端杀毒工作蚕食殆尽。

事实证明，安全漏洞往往出现在你早已司空见惯的工作习惯中，是让病毒进入到网络之后再绞杀？还是将病毒斩杀在入口处，建造一个相对安全的内网呢？面对这样的选择，安阳市工商行政管理局信息中心选择了后者。IT 工程师不但利用趋势科技提供的 IWSA 有效提升了网络的防护能力，同时也把自己从繁杂的终端防毒维护中解脱了出来。

网关一旦失守 终端维护成本过大

据了解，安阳市工商行政管理局信息化建设起步较早，发展至今，内部公文流转、监测等级、综合业务系统等等都与网络密不可分，而且终端用户的数量已经达到了千台之多。作为主管安阳市市场监督管理和行政执法工作的一级机构，安阳市工商行政管理局每个下属单位的网络连接方式较为复杂，不但直属科室、区县分局、工商所众多，而且负责每个子网运行的 IT 人员安全管理技能水平也参差不齐。随着互联网 Web 访问环境的不断恶化，在这个庞大的工商网络系统中，终端安全的维护问题也开始随之凸现。

安阳市工商行政管理局信息中心的工程师张先生表示：“我们已经要求所有的用户都安装了桌面防病毒软件，但病毒事件还是继续困扰着普通用户和信息中心的同事。面对现在 Web 病毒成倍增长的环境，我们不但对原有的防火墙进行了策略调整，还调整上网行为管理设备中地址库的更新频率，增加了内部计算机防病毒软件的客户端检查策略，但仍无法避免由于感染病毒而导致一部分终端或子网暂时性瘫痪现象的发生。”据介绍，安阳市工商行政管理局信息中心只有 4 名工程师，不但要负责业务系统问题、软件问题、硬件问题、网络问题，

还包括客户端问题等等。一旦客户端出现中毒现象，相关的杀毒、系统恢复工作占用了信息中心大量的人力时间。维护客户端的工作占到了时间成本的 50%~60%甚至更高，因此，如何在网关层面上加强防毒措施，减少客户端中毒的机率，这项工作已经到了刻不容缓的阶段。

IWSA 测试上线 第一时间多只木马被“斩头”

近期，随着安阳市工商行政管理局下属单位网络出口统一工作的落实，80 多家下属工商所都完成了到信息中心汇总的专线连接。由于网络的出口得到了汇聚统一，这样便为 Web 安全网关发挥最大功效提供了物理条件。安阳市工商行政管理局信息中心的高吉林主任表示：“经过对云安全产品市场的了解，以及对最新威胁防护知识的学习，我们都意识到，防御体系不但需要功能丰富的安全产品，更需要主动性防毒架构来承载，避免终端接触到病毒源头，利用云安全提供的强大平台，这样的防护设计思路才是我们想要的。出于对趋势科技产品品牌的信任，以及有别于传统防毒代码的杀毒架构的设计，都是我们最终选择了 IWSA 的原因。”

在考查了很多网关产品之后，由于趋势科技的 IWSA 可以透明的部署在网关处，不用修改现在网络结构。因此，安阳市工商行政管理局决定将其部署在信息中心总部的 Internet 出口处进行测试，弥补防火墙和上网行为管理系统只能针对连接进行限制的策略，把诸如“网站挂马”这样的威胁都消灭在网关处。在 IWSA 刚刚安装上线的一分钟内，通过 IWSA 1500 的监控发现，就成功的拦截阻止住了 20 余次病毒入侵。信息中心的工程师纷纷表示，之前我们在聆听趋势科技的产品介绍时，虽然有些疑虑，但实际的效果让我们之前的疑虑全部打消了。在连续 24 小时不间断运行的同时，信息中心对终端用户实际体验进行了大量的测试，IWSA 并没有对正常业务往来造成影响，相反上网的速度明显加快，这是由于大量恶意链接被有效阻拦，且木马和病毒侵占的流量被基本消除的结果。

云安全 降低管理成本的明智之选

水能载舟亦能覆舟，一方面员工在工作中可以通过互联网获取有用资源，提升工作质量并降低工作成本；但另一方面，互联网上数不胜数的恶意代码随时都可能进入终端，而病毒或木马一旦爆发就会严重降低工作效率。在正式部署了 IWSA 1500 之后的几个月里，安阳市工商行政管理局不但为员工创造了良好上网条件，同时也对互联网应用起到了合理的控制和管理。

之前，许多下属单位中一些杀毒软件的病毒库更新不及时，无法抵御最新病毒的入侵，对不同下属单位在同一时间实施统一的安全策略难度非常大，沟通、实施以及检查的成本非常高，

经常出现管理漏洞。而现在利用 IWSA 的云安全特性，让各级单位在第一时间应用最新的趋势科技的智能防护网络的防护智能和威胁数据库，这样不仅降低了终端的防护压力，也让 IT 人员从安全策略的管理的困扰中解脱了出来。高吉林主任指出：“嵌入云安全技术的趋势科技产品与解决方案不仅具备了 Web 威胁数据库为依据的信誉评级技术，还为我们日常管理提供了详细的安全报表和预警功能。这些独特的云安全防护技术，可以为用户提供实时保护，防范最新的 Web 威胁。在逐步了解趋势科技安全威胁解决方案的内容之后，我们准备在网络层试用 TDA 等威胁发现设备，从而建立起层次更加鲜明、更加细化的安全防范体系。”

###

关于趋势科技 (Trend Micro)

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,200 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。